State of New Hampshire

Department of Safety

Division of Fire Standards and Training and Emergency Medical Services
Richard M. Flynn Fire Academy
98 Smokey Bear Blvd., Concord, New Hampshire
Mailing Address: 33 Hazen Drive, Concord, New Hampshire 03305-0002

John J. Barthelmes
Commissioner

Richard A. Mason
Director

MEMORANDUM

TO: NH EMS Units
NH EMS Regional Chairs
NH EMS Hospital Coordinators

FROM: Michael Schnyder, BS, SSBB, NREMT-P
FST & EMS
Bureau of EMS

RE: Verifying Optimal Security Setting for Your Internet Browsers

DATE: April 14, 2008

On behalf of the New Hampshire Department of Safety, Division of Fire Standards and Training and Emergency Medical Services (FST & EMS), we would like to take this opportunity to notify you about updating your TEMSIS security settings.

The majority of the Trauma and EMS Information System (TEMSIS) users create patient care reports using the Internet-based solution. Quite recently a number of news events have come into the light about the diligence required to protect private information. After an expedited review of TEMSIS' practices, we requested our software vendor, ImageTrend, to develop a "best practices" document on Internet Browser settings.

We now ask for each EMS or Fire agency, hospital, and anyone who uses TEMSIS to set their Internet Browsers to the maximal level to protect against potential threats. To assist everyone with this process, we took ImageTrend's work and divided it into three components:

- Best Practices for Microsoft Internet Explorer
- Best Practices for Mozilla Firefox
- An "expert level" document for those organizations with an established IT staff.

These documents will be located both on the TEMSIS (**www.nhtemsis.org**) and EMS Bureau's websites (**http://www.nh.gov/safety/divisions/fstems/ems/forms.html**).

Please also take the time to review your overall current security practices to ensure that protected health information (PHI) is at its the best. This ranges from the simple idea of not leaving a drop-off form on a counter to storing PHI in secure location.

If you have any questions about Internet browser security practices, please contact ImageTrend at: 1.888.469.7789. For other questions, please contact the Bureau's Research & Quality Management Section at 603-223-4226.

Browser Security Recommendations

Any computer that is or may be used to access patient data should conform to industry best practices standards for security. Outlined below are simple changes to your Web browser recommended by ImageTrend that increase the level of protection of data, and improve the security on your computer.

Microsoft Internet Explorer Configuration

The following recommendations are specific to Internet Explorer 7; however, previous versions of Internet Explorer should follow similar guidelines as much as possible.

- Temporary Internet Files and History Settings
    - Set the browser to check for newer versions of stored pages every time the user visits the Web page.
    - Change the number of days that Web pages are kept in the browsing history.
      HINT: If you don't want a Web page history kept, set the number of days to 0.
- Frequently delete the browsing history.
- From advanced security settings, select the checkboxes beside the options for *Do not save encrypted pages to disk* and *Empty Temporary Internet Files folder when browser is closed*.
- Do not allow AutoComplete for usernames and passwords on forms.
- Always allow pop ups from the State Bridge.
- Set your browser security to High.
- Add safe websites to trusted sites: allow access to sites that begin with *http:* if necessary.

Fundamental Mozilla Firefox Configuration

- Temporary Internet Files and History Settings
    - Do not remember visited pages.
    - Always clear all private data when Firefox is closed.
- Do not remember passwords.
- Allow pop ups from the TEMSIS site.

Additional Computer Security Recommendations

- Make sure you have the latest Windows and browser updates, including anti-virus definitions.
  NOTE: This includes having the most up-to-date browser.
- Make sure to log out of websites and close all of your browser windows when finished or away for an extended amount of time.
- Install anti-virus software.
- Install anti-spyware software.